Statement of Pending Claims:

Claims 16-52 and 59-86 are pending. Claims 1-15 and 53-58 were previously cancelled in connection with a restriction requirement.

REMARKS/ARGUMENTS

Rejections under 35 U.S.C. § 102

§ 102 Rejections based on U.S. Patent 5,748,783 ("Rhoads")

Claims 16-22, 25-27, 29, 31-40, 42, 43, 45-52, 59-64, 66-86 stand rejected as allegedly anticipated by U.S. Patent No. 5,748,783 issued to Rhoads (thereafter "Rhoads"). See Page 2 of the Office Action.

Claims 16-20, 22, 25, 27, 31, 33, 34, 37, 38, 42, 43, 45-52, 59, 62-64, and 66-86

In order for a reference to anticipate a claim, the reference must disclose each and every limitation of the claimed invention, either expressly or inherently, such that a person of ordinary skill in the art could practice the invention without undue experimentation. See Atlas Powder Co. v. Ireco Inc., 190 F.3d 1342, 1347, 51 USPQ2d 1943, 1947 (Fed. Cir. 1999); In re Paulsen, 30 F.3d 1475, 1479, 31 USPQ2d 1671, 1673 (Fed. Cir. 1994). Independent Claim 16 [emphasis added] recites, *inter alia*, "[a] method of **generating a random key for applying a digital watermark** to a content signal, the method comprising the steps of: **generating a random sequence of binary numbers**; and **generating information describing the application of the random sequence to the content signal**, wherein the information comprises a sample window size, a signal encoding level, and at least one of the following two groups: time delimiters describing segments of the content signal; frequency delimiters describing frequency bands of the content signal." The Section 102 rejection of Claim 16 is improper for at least the reason that Rhoads fails to disclose "generating a random key for applying a digital watermark." Assuming, *arguendo*, that Rhoads' "... robust information coding wherein several random digital signals

2

are generated..." "... meets the limitations generating a random sequence of binary numbers for applying a digital watermark to a content signal", as the Examiner asserts at Office Action Page 2, Rhoads significantly fails to disclose the additional step of "generating information describing the application of the random sequence to the content signal" as required by Claim 16, and, for this additional reason, the 102 rejection should be withdrawn.

The Examiner asserts that "... Rhoads discloses a method for robust information coding wherein several random digital signals are generated to be (Fig. 2) embedded into an input source signal that could be an image, or video to produce a watermarked signal (Abstract), which meets the limitations generating a random sequence of binary numbers for applying a digital watermark to a content signal" Office Action at Page 2. First, Rhoads describes equivalences between "signature codes", "invisible signatures", and "signatures" reciting that they "... often refer specifically to the composite embedded code signal as described early on in this disclosure," Rhoads at Col. 37 ll. 30-36. These may *arguably* relate to "a random sequence of binary numbers" but there is no additional functionality coupled with the alleged "random sequence" for purposes of "generating a random key for applying a digital watermark". Second, it may be that the alleged "random sequence" of Rhoads is simply the "signature codes", "invisible signatures", "signatures", or "composite embedded code signal" he recites as being equivalent terms. However, Rhoads teaches away from generating "random keys", and more importantly, "generating information describing the application of the random sequence to the content signal." The significance is in the functionality of the claimed invention, namely "generating a random key for applying a digital watermark to the content signal." Three of the claim elements: "random key", "digital watermark", and "content signal" make possible watermarking which is difficult, or computationally infeasible to guess (e.g., the "random key"), while also enabling content owners to separately store their original unwatermarked signals without having to expose them again. More about this significant feature below.

Rhoads teaches away from a "random key" which includes the step of "generating information describing the application of the random sequence to the content signal", by requiring "[t]he original signal, the N-bit identification word, and all N individual embedded code signals are then stored away in a secured place" Rhoads at Col. 5 ll. 10-13, for subsequent detection or decoding, see Rhoads at Figure 3; Col. 8 ll. 41-67 – Col. 9 ll. 1-62. As a means of securing a digital signal the requirement of at least comparing the original for purposes of detection or decoding, as Rhoads discloses, is wasteful from a computational perspective and, in effect, significantly undermines any supposed security. One of ordinary skill in the art can readily appreciate that the need to distribute the original signal (necessary for Rhode's comparison step) exposes the unwatermarked data to the risk of copying. Practically speaking, why copy a modified signal if you can obtain access to the original signal? This is why the Applicant's invention offers a significant advantage over the alleged security taught by Rhodes.

Next, the Examiner asserts that "... Figs. 9A & 9B give an example of what the waveform of an industry standard noise second may look like, both in the time domain and the frequency domain, this meets the limitation of generating information describing the application of the random sequences to the content signal and the information being of two groups: time delimiters describing segments of the content signal; frequency delimiters describing frequency bands of the content signal" Office Action at 2. Rhoads does not teach "generating information describing the application of the random sequence to the content signal," and instead argues for acceptance of "standardized noise signatures", Rhoads at Col. 28 ll. 31. Further arguing that contrary to the use of random keys for applying a digital watermark, "standardized noise signatures" should be adopted. Rhoads, at Col. 11 ll. 1-8 [emphasis added]: **"The fullest expression of the present system will come when it becomes an industry standard** and numerous independent groups set up with their own means or `in-house` brand

4

of applying embedded identification numbers and in their decipherment. Numerous independent group identification will further enhance the ultimate objectivity of the method, thereby enhancing its appeal as an industry standard." Again, functionality differentiates the claim limitation of the instant invention. If there were "standardized noise signatures", there would be no need for "generating information describing the application of the random sequence to the content signal."

That Rhoads argues for such "standardization" and requires "[t]he original signal, the N-bit identification word, and all N individual embedded code signals are then stored away in a secured place" Rhoads at Col. 5 ll. 10-13, for purposes of detection or decoding, is antithetical to random key creation including the step of "generating information describing the application of the random sequence to the content signal." This information is necessary for the random key to have functionality. There is a parallel with comparisons between symmetric encryption, where one key performs encryption and decryption, and asymmetric encryption, where a private key performs encryption and a public key performs decryption. As argued here, Rhoads would likely advocate that all of his encoded messages be "standardized" and compared to original unencoded messages. Thus, there is no need to generate keys since originals would be available for detection and decoding. Because Rhoads' alleged "random sequences" have no functionality beyond identification, they are not disclosed as requiring the additional step of "generating information describing the application of the random sequence to the content signal." Rhoads argues [emphasis added] "… if the suspect image is indeed a copy of our original, the embedded 32-bit resulting code **should match** that of our records…" Rhoads at Col. 9 ll. 46-49.

That a "unique identification code" may be made more secure by generating a "random key" including "generating information generating information describing the application of the random sequence to the content signal", as taught by the instant invention, is a significant benefit over Rhoads,

5

and provides security benefits. As argued previously, as a means of securing a digital signal the requirement of at least comparing the original for purposes of detection or decoding, as Rhoads discloses, is wasteful from a computational perspective and, in effect, significantly undermines any supposed security. One of ordinary skill in the art can readily appreciate that the need to distribute the original signal (necessary for Rhode's comparison step) exposes the unwatermarked data to the risk of copying. Practically speaking, why copy a modified signal if you can obtain access to the original signal? This is why the Applicant's invention offers a significant advantage over the alleged security taught by Rhodes.

Next, the Examiner asserts "... Col. 25, lines 30-60 discusses the resolution parameters in the embedding process, which meets the limitation of the sample window size," Office Action at Page 3. Contrary to the Examiner's assertion "sample window size" is not taught, encryption of the "embedded codes" is taught. In fact, Rhoads discloses that:

> Thus we find that 50 of these independent embedded codes will amount to a few Megabytes. This is quite ['a'] reasonable level to distribute as a 'library' of universal codes within the recognition software. Advanced standard encryption devices could be employed to mask the exact nature of these codes if one were concerned that would-be pirates would buy the recognition software merely to reverse engineer the universal embedded codes. The recognition software could simply unencrypt the codes prior to applying the recognition techniques taught in this disclosure Rhoads at Col. 25 II. 50-60.

This teaches away from "information describing the application of the random sequence to the content signal, wherein the information comprises a sample

6

window size" since the encryption is applied to a library of codes. The Applicants' invention is directed at "a sample window size" of the "content signal" to enable "generating information describing the application of the random sequence to the content signal." In this manner, a variety of encoding, and by extension decoding, operations derived from a "random key" are made possible. This may include for instance differences in "sample window sizes" for better robustness, security, or imperceptibility of the encoding or differences in "content signals", including: images, audio, video content, and combinations that are multimedia in nature.

Independent Claim 34 discloses "generating a random or pseudo-random sequence of binary numbers", similar to Claim 16's "generating a random sequence of binary numbers." Claim 34, and claims depending therefrom, require the additional steps of (1) "associating with the random or pseudo random sequence, one or more references to encoding functions for encoding at least one watermark into a content signal" and (2) "embedding at least one watermark into a content signal using the referenced encoding functions." As argued above, Rhoads' alleged "random sequence" has no functionality: it is arguably the "N-bit identification word" which can be used for identification. Assertions that Rhoads' "random sequence" includes the steps of associating the sequence with "encoding functions" and subsequent "embedding" based on the "reference encoding functions" is improper. Claim 34 is allowable for at least the reasons discussed above in connection with claim 16, namely, that while Rhoads may *arguably* disclose "a random sequence of binary numbers," Rhoads does not disclose any additional functionality coupled with the alleged "random sequence" for purposes of embedding a digital watermark. Second, it may be that the alleged "random sequence" of Rhoads is simply the "signature codes", "invisible signatures", "signatures", or "composite embedded code signal" he recites as being equivalent terms. However, Rhoads teaches away from associating the sequence with the encoding function. The significance is in the functionality of the claimed invention, namely "associating with the random or pseudo random

7

sequence, one or more references to encoding functions for encoding at least one watermark into a content signal."

Independent Claim 47, extends the functionality of the Applicants claimed invention[s] to include "embedding a plurality of digital watermarks into a content signal" based on at least the steps of (1) "associating each of the random or pseudo random sequences with one or more references to encoding functions for encoding watermarks into a content signal, and with each of the plurality of digital watermarks to be embedded" (2); "and embedding each of the plurality of digital watermarks into the content signal using the referenced encoding functions associated with the respective digital watermark". Claim 47 is patentable over Rhoads for at least the reasons discussed above in connection with Claim 34 and Claim 16. Claim 47 is patentable over Rhoads for the additional reason that Rhoads does not appear to teach the use of multiple watermarks. Rhoads fails to disclose "random sequences with one or more encoding functions" and arguably relies on a single "N-bit identification word" which may allegedly be a *single* "random sequence" per signal, not multiple watermarks per content signal as required by Claim 47 (and the claims that depend therefrom). This additional benefit over Rhoads allows for multiple parties to embed multiple watermarks governed by separate "associated encoding functions" that may be independently random from each other, based on the associated "random sequence[s]". This may increase security by allowing less important watermarks to be governed by simpler encoding functions and also enables improvements to encoding by changing the "random sequences" with different "references to encoding functions" so that upgrades may be handled without replacing the entire watermarking system. Rhoads does not appear to teach the use of such multiple watermarks, nor the advantages associated therewith. The Applicants teach the importance of upgradeability in the Specification, and the computational benefits of using "random sequences" for encoding and decoding purposes without needing to introduce the original unwatermarked signal to potentially malicious parties, as is inherent to Rhoads.

Similarly, independent Claim 59, and all claims that depend therefrom, address devices for (1) "a function generator which is capable of generating a plurality of encoding functions"; (2) "an association device to associate one of said at least one sequence of random binary numbers with at least one of said plurality of encoding functions and with a watermark generated by the watermark generator." As argued above, Rhoads' alleged "random sequence" is not associated with "information describing the application of the random sequence to the content signal", nor more particularly, "a function generator" for purposes of watermarking a content signal. Because Rhoads relies on the uniqueness of his "N-bit identification word" his "binary sequences" are not functional in a manner parallel to the instant invention[s] claim limitation. In addition to the reasons discussed in accordance with Claim 47, Claim 59 is allowable for the additional reason that Rhoads fails to disclose the "association device to associate" a sequence of random binary numbers to an encoding function with a watermark generated by the watermark generator. For at least the reasons discussed above in connection with Claims 16 and 34, Claim 59 is allowable.

Independent Claim 70, and all claims that depend therefrom, requires at least the following steps: (1) "a watermarking key generator which generates a watermarking key using a sequence of random binary numbers generated by the random number generator and using input from the function generator" and (2) "an encoding device to encode a watermark generated by the watermark generator into the content signal using a watermarking key generated by the watermarking key generator." Rhoads' alleged "random sequence" is not coupled to a "function generator", nor does Rhoads mention "watermarking" in connection with "key generation". As disclosed previously, Rhoads relies on distribution of "[t]he original signal, the N-bit identification word, and all N individual embedded code signals are then stored away in a secured place" Rhoads at Col. 5 ll. 10-13, for detection or decoding, see Rhoads at Figure 3; Col. 8 ll. 41-67 – Col. 9 ll. 1-62, teaching away from generating a "watermarking key". Using watermarking

keys has significant security benefits over Rhoads, and enables individual content owners to generate and maintain their own watermarking keys for protecting their own content signals. No industry standardization, as apparently desired by Rhoads, is necessary. In fact, some of the benefits of public key cryptography, as known to those skilled in the art, depend on the ease at which key distribution can be handled. The instant invention offers similar benefits not disclosed by Rhoads. Thus, Claim 70 is allowable over Rhoads for at least the reasons discussed in connection with Claim 59. Claim 70 is allowable over Rhoads for the additional reason that Rhoads fails to disclose a watermarking key generator in accordance with the limitations of Claim 70.

Independent Claim 79, and all claims that depend therefrom, split "a digital watermark encoder" from "a digital watermark decoder". This is noticeably absent from Rhoads as he advocates use of at least the original signal to be used for detection and decoding of "N-bit identification word[s]". This split can then rely on (1) "a watermarking key that encodes a watermark into a content signal using a random or pseudo-random binary sequence" and (2) "an encode and decode pair associated with the watermarking key". Again, Rhoads fails to disclose a "random or pseudo random sequence" that has this type of functionality. This improves key management for the "watermarking key" as there would be "an encode and decode pair" for which encoders and decoders could be logically separated. Rhoads discloses no such functionality and thus the instant invention is a significant improvement over Rhoads. Regardless of whether Rhoads discloses an "encode key" he does not disclose a "decode key" because his decoding relies on the "original signal", as argued previously. Claim 79 is patentable over Rhoads for this additional reason that Rhoads fails to disclose a "decode key" in accordance with the limitations of Claim 79.

For at least these reasons discussed above, the independent claims, namely, Claims 16, 34, 47, 59, 70 and 79 are patentable over Rhoads. The rejected claims that depend from the independent claims, namely, 17-20, 22, 25,

27, 31, 33, 37, 38, 42, 43, 45-46, 60-52, 59, 62-64, and 66-69, 71-78, and 80-86, are patentable over Rhoads for at least the same reasons that their respective independent claims are patentable. Accordingly, Applicants request that the Examiner withdraw the 102 rejections for Claims 16-20, 22, 25, 27, 31, 33, 34, 37, 38, 42, 43, 45-52, 59, 62-64, and 66-86.

102 Rejections Directed to Selected Dependent Claims

Additional and independent reasons why certain dependent claims are allowable are recited below:

Claim 21

Applicants respectfully disagree with the Examiner's assertion that "... Rhoads discloses that there can be more than one content stream samples (Col. 15, lines 54-63)" Office Action at Page 3. The cited passage refers to a single "input sample" for which "... each input sample (i.e. look-up table address), the table provides a corresponding 8-bit digital output word," Rhoads at Col. 15 ll. 59-61. It is not clear how the Examiner is interpreting the reference to mean the same as Claim 21's limitation of "... providing at least two sample streams of the content signal for selection ...". In fact, Rhoads goes on to say, "The addition or subtraction of the scaled noise signal in accordance with the bits of the code word effects a modulation of the input signal which is generally imperceptible" Rhoads at Col. 16 ll. 40-42. Multiple content streams do not appear to be contemplated. Providing multiple input streams for which multiple random sequences or watermark keys can be associated is absent in Rhoads' disclosure. As argued previously, the additional enabling step of "generating information describing the application of the random sequence to the content signal" is also absent in Rhoads. The improvements in Claim 21, for instance, enable encoding of audio and video streams in a multimedia content signal based on functions that are specific to audio and video coding schemes, respectively. It would also enable watermarking based on "random sequences" or associated "random keys" with hierarchy for different distribution schemes or access by different

entities in a variety of distribution scenarios. One party may own rights to the audio stream of a combination video and audio, for instance. For these reasons, Claim 21 is patentable over Rhoads. Applicants request that the Examiner withdraw the Section 102 rejection of Claim 21.

Claim 32

Applicants respectfully disagree with the Examiner's assertion that "… Rhoads discloses being able to locate the watermark information signal in the content signal and verify the watermark information as the very information that was embedded earlier (Col. 8, line, 42 – Col. 9, line 62)" The additional claim limitations include both (1) "generating a watermark information signal comprising watermark synchronization information to help locate a watermark in the content signal and information to **help assess the validity of said watermark**" and (2) "placing the watermark information signal within the content signal so as to **not interfere with any digital watermarks embedded in the content signal**". These additional steps require first "generating information describing the application of the random sequence to the content signal" (Claim 32 depends from Claim 16) while Rhoads relies on at least the "original signal" and the "N-bit identification word" for comparison. Additionally, by not interfering with "any digital watermarks embedded in the content signal", validity can be determined without relying on an "original signal" as is inherent to Rhoads. However, Rhoads does not express confidence about his "N-bit identification word" [emphasis added] "… if the suspect image is indeed a copy of our original, the embedded 32-bit resulting code **should match** that of our records…" Rhoads at Col. 9 ll. 46-49. A simpler approach is to compare the original to the suspect copy and make a human decision about whether it is a copy – this simple approach carries security flaws as argued previously in subjecting the "original signals" to access by third parties. Rhoads also apparently asserts that industry standardization is preferable to addressing potential interference between digital watermarks. But, as argued previously, one of ordinary skill in the art can readily appreciate that

the need to distribute the original signal (necessary for Rhode's comparison step) exposes the unwatermarked data to the risk of copying. Practically speaking, why copy a modified signal if you can obtain access to the original signal? This is why the Applicant's invention offers a significant advantage over the alleged security taught by Rhodes. Because of the above recited claim limitations, Claim 32 is patentable over Rhoads. For these reasons, Claim 32 should be allowed. Applicants request that the Examiner withdraw the Section 102 rejection of Claim 32.

Claims 35, 36 and 39

Applicants respectfully disagree with the Examiner's assertion that "... Rhoads discloses using alphanumeric codes in the encoding functionality (Col. 34, lines 48-67)" Rhoads actually discloses that "alphanumeric codes" are used for identification not functionality as per the Applicants' disclosures and claim limitations. "It is desirable in some applications for the N-bit identification word to actually signify names, companies, strange words, messages and the like" Rhoads at Col. 34 ll. 48-50. This does not meet the limitations of Claim 34, from which Claims 35, 36 and 39, specifically: (1) "associating with the random or pseudo random sequence, one or more references to encoding functions for encoding at least one watermark into a content signal" and (2) "embedding at least one watermark into a content signal using the referenced encoding functions." Rhoads fails to disclose associating functionality to his alleged "random sequence" as argued previously. For instance, Claim 35 "wherein said one or more references is selected from the group consisting of: integer indices that reference chunks of computer code; alphanumeric strings which name software modules or code resources; and memory addresses of memory locations wherein software programs reside in a computer memory"; Claim 36 "wherein said one or more references comprise alphanumeric strings which identify software modules that can be used to embed a watermark into a content signal"; and Claim 39 "wherein said one or more decoding references comprise

alphanumeric strings which identify software modules that can be used to extract a watermark from a content signal". That Rhoads' alleged "random sequences" lack functionality, what Rhoads' "N-bit identification word[s]" are apparently used for is identification, alone. The improvements offered by Claims 35, 36 and 39 for optimizing the functionality of the Applicants' "random or pseudo random sequences" for both "embedding digital watermarks" and "extracting digital watermarks" are realized. These are significant benefits over Rhoads to improve security and computational processing not just compression of "alphanumeric messages", as per the teachings of Rhoads. For at least these reasons, Claims 35, 36 and 39 are patentable over Rhoads. Applicants request that the Examiner withdraw the Section 102 rejection of Claims 35, 36 and 39.

Rejections under 35 U.S.C. § 103

In order to "establish a prima facie case of obviousness, three basic criteria must be met." MPEP § 7.06.02(j). First, there must be some motivation or suggestion to modify the reference or to make the proposed combination. Second, there must be a reasonable expectation of success. "The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on the applicant's disclosure." MPEP § 2142 (citing In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). Third, the combined references must teach or suggest all claim limitations.

The Examiner has failed to establish a prima facie case of obviousness to the extent that there is no motivation or suggestion to make the proposed combinations of the references as directed by the Examiner. According to the MPEP, [i]n order to support a conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention obvious in light of the teachings of the references. MPEP 2142 (citing Ex parte Clapp, 277

14

USPQ 972, 973 (Bd. Pat. App. & Inter. 1985)) (emphasis added). Further, "[w]hen the motivation to combine the teachings of the references is not immediately apparent, it is the duty of the examiner to explain why the combination of teachings is proper." MPEP 2142 (citing Ex Parte Skinner, 2 USPQ2d 1788 (Bd. Pat. App. & Inter. 1998)).

The Federal Circuit has recently emphasized the importance of providing evidence of motivation to combine in Winner Int'l Royalty Corp. v. Ching-Rong Wang, 202 F. 3d 1340, 1348-49 (Fed. Cir. Jan. 27, 2000). "Although a reference need not expressly teach that the disclosure contained therein should be combined with another . . . the showing of combinability, in whatever form, must nevertheless be 'clear and particular.'" Winner, 202 F. 3d at 1348-49 (citations omitted). Further, the "absence of such a suggestion to combine is dispositive in an obviousness determination." Gambro Lundia AB v. Baxter Healthcare Corp., 11 F.3d 1573, 1579 (Fed. Cir. 1997).

Applicants submits that the Examiner has not satisfied his initial burden of providing "clear and particular" evidence of motivation to combine for any of the proposed combinations of references. Instead, it appears that the Examiner has simply identified references that allegedly disclose the elements of the claim, and has combined them. Even assuming *arguendo* that the references contained all elements of the claimed invention, it is still impermissible to reject a claim as being obvious simply "by locating references which describe various aspects of a patent applicant's invention without also providing evidence of the motivating force which would impel one skilled in the art to do what the patent applicant has done." Ex parte Levengood, 28 USPQ2d 1300, 1303 (Bd. Pat. App. & Inter. 1993) (emphasis added).

§ 103 Rejections Based on Rhoads and Menezes as applied to Claims 23 and 24

Claims 23 and 24 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Rhoads in view of Menezes. The Examiner asserts that "... Menezes discloses generation of a random key using random strings that are hashed and run through a DES algorithm...", Office Action of Page 4. Claims 23 and 24 depend from Claim 16. Applicants disclose "random sequence" generation to "watermark" a content signal by forming a "random key" for "applying a digital watermark".

The combination of Menezes and Rhoads fails to disclose "concatenating the extracted least significant bits to form a random key sequence" (Claim 23 element) which then interacts with a "content signal" in such a manner as to result in a digitally watermarked "content signal". The enabling step of "generating information describing the application of the random sequence to the content signal" (Claim 16 from which Claim 23 and 24 depend) does not result from the combination of the references. "Random keys", as taught by Menezes and known in the art cryptography, do not imperceptibly change a content signal, they yield an encrypted signal. Assuming, *arguendo*, Menezes taught "random sequences" similar to those of the Applicants, the functionality of said "random sequence" would be for encryption *not* steganographic encoding.

Rhoads teaches generation of an "N-bit identification word", this alleged "random sequence" lacks the functionality of the Applicants' "random sequence" for at least the reason that the enabling step of "generating information describing the application of the random sequence to the content signal" is not disclosed by Rhoads. Neither Menezes, nor the combination of Rhoads with Menezes, discloses this claim element. Menezes' alleged "random key" is directed at encryption, which would render the "N-bit identification word" of Rhoads encrypted not "watermarked". Adding Rhoads would be improper since his "N-bit identification word" is *not* a "random sequence". The combination teaches that Rhoads with Menezes' "random bit generator" would logically result in a "N-bit identification word" that has "random bits"-- not "a random key for

applying a digital watermark to a content signal" including the enabling step of "generating information describing the application of the random sequence to the content signal".

Rhoads' own descriptions may also yield significant additional reasons why an "N-bit identification word" should *not* be considered a "random sequence". Rhoads argues that his "N-bit identification word" may be compressed, Rhoads at Col. 34 ll. 47 – Col. 35 ll. 3. If the "N-bit identification word" is compressible, it may not, by definition, be a "random sequence" as per Menezes and teachings by those skilled in the art of cryptography. As Menezes points out: "[t]he basic idea behind Maurer's universal statistical test is that it should not be possible to significantly compressed (without loss of information) the output sequence of a random bit generator", Menezes at Page 183 (Section 5.4.5).

There is no motivation to combine these two references as claimed in accordance with the claimed invention. The Examiner is using the instant invention as a roadmap to combine the references. Applicants therefore request the Examiner withdraw the Section 103 rejections of Claims 23 and 24 (which depend from Claim 16).

§ 103 Rejections Based on Rhoads and Shur as applied to Claim 28

This Application is a continuation pursuant to 37 C.F.R § 1.53(b) of Application Serial Number 08/674,726 filed July 2, 1996, as indicated by the preliminary amendment dated April 7, 2000. Shur is not prior art because it's relevant date is subsequent to the July 2,1996 filing date of this application's parent application. Therefore, Shur cannot appropriately be combined with Rhoads. Per the Examiner's own analysis, Rhoads alone does not make obvious Claim 28. Accordingly, Claim 28 is allowable.

§ 103 Rejections Based on Rhoads and Koopman as applied to Claims 30, 41, and 65

Claims 30, 41 and 65 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Rhoads in view of Koopman. The Examiner asserts that "... Koopman discloses a random number generation process wherein a random sequence is concatenated with certain values of an incoming signal and subsequently encrypted (Abstract)." Koopman does not disclose concatenation with a "random key for applying a digital watermark to a content signal." As argued previously, Rhoads does not teach a "random sequence" as per the Applicants' disclosure; instead, Rhoads teaches an "N-bit identification word".

Combining Rhoads and Koopman would logically result in encrypting the "N-bit identification word". Rhoads and Koopman would not result in "encrypting a concatenated string" including "the random sequence" and the "generated information" as would be necessary to render obvious Claims 30, 41, and 65. Applicants' disclosure is directed at securing a "random sequence" or "random key" after it has been used to watermark a "content signal". This combinatorial step of Applicant's invention increases the security of the Applicants' "random key[s]". Rhoads, as has been argued above, does not rely on "random sequences" or "random keys" for detection or decoding, but instead requires at least the "original signal" and "N-bit identification word" to recover the changes. Thus, encrypting the N-bit identification word does not yield the claimed invention, and therefore the combination does not render the claims obvious.

The reliance upon Koopman's does not produce the missing element. Koopman's "random number generation" process results in an encrypted "key word which is transmitted with the fob ID," Koopman at Abstract. As per Koopman, encrypting the alleged "random sequence" of Rhoads would apparently result in an encrypted "N-bit identification word". Applicants' disclosed "random sequence", as argued previously, includes the enabling steps of "generating information describing the application of the random sequence to the content signal" (as stated in Claim 16 from which Claim 30 depends); "associating with the random or pseudo random sequence, one or more

18

references to encoding functions for encoding at least one watermark into a content signal" (as stated in Claim 34 from which Claim 41 depends); and, "an association device to associate one of said at least one sequence of random binary numbers with at least one of said plurality of encoding functions and with a watermark generated by the watermark generator" (as stated in Claim 59 from which Claim 65 depends). Rhoads' alleged "random sequence" as well as Koopman's encryption scheme each lack the claimed functionality and the enabling steps (as required by each of the relevant claims). Accordingly, the combination of Rhoads and Koopman fails to yield the claimed inventions. For this reason, the 103 rejections should be withdrawn.

Furthermore, neither reference teaches that the other may be combined in accordance with the requirements of the claim. In other words, there is no express motivation to combine these two references as required by the terms of the claimed invention. The Examiner is using the instant invention as a roadmap to combine the references, which is impermissible. Applicants therefore request the Examiner withdraw the Section 103 rejections of Claims 30, 41, and 65 (which depend from Claim 16, 34, and 59 respectively).

§ 103 Rejections Based on Rhoads and Shur as applied to Claim 45

This Application is a continuation pursuant to 37 C.F.R § 1.53(b) of Application Serial Number 08/674,726 filed July 2, 1996, as indicated by the preliminary amendment dated April 7, 2000. Shur is not prior art because it's relevant date is subsequent to the July 2,1996 filing date of this application's parent application. Therefore, Shur cannot appropriately be combined with Rhoads. Per the Examiner's own analysis, Rhoads alone does not make obvious Claim 45. Accordingly, Claim 45 is allowable.

Conclusion

Applicant maintains that this application is in condition for allowance, and such disposition is earnestly solicited.

19

It is believed that no other fees are required to ensure entry and consideration of this response.

Respectfully submitted,

Date: June 14, 2004   By: _Scott Moskowitz_____

Scott A. Moskowitz